CHAPTER 3

SYSTEM CONTROL REQUIREMENTS

A. INTRODUCTION

It is through the use of a set of clearly defined objectives that an effective and efficient management controls program is implemented. The requirements constitute a core around which a plan of action can be developed. The 55 control requirements are grouped under the following four categories:

- application controls
- general controls
- administrative controls
- required system functions

B. SYSTEM CONTROL REQUIREMENTS

- APPLICATION CONTROLS

1. Transactions are authorized - the information entered into the system must be authorized by management for entry.

2. Transactions are valid - the information system must process only data that represent legitimate events.

3* Information is complete - all valid data, and only those data, are to be processed by the information system.

4. Information is accurate - data must be free from error during all phases of processing, within defined levels of tolerance.

5. Information is timely - data must reflect the correct cycle, version, or period for the processing being performed. Financial management data shall be recorded as soon as practical after the occurrence of the event, and relevant preliminary data shall be made available promptly to managers after the end of the reporting period.

6. System and data are secure - the data files, computer program, and equipment must be secure from unauthorized and accidental changes, unauthorized disclosure and use, and physical destruction. Detective and corrective controls may also apply depending on the sensitivity and/or classification of the data.

7. System is auditable - an information trail must exist that" establishes individual accountability for transactions and permits an analysis of breakdowns in the system and other anomalies.

- GENERAL CONTROLS

8. System controls exist - for each information system, the controls system should ensure that appropriate safeguards are incorporated into the systems, tested before implemental ion, and tested periodically after implementation.

9. Five-year system plan developed - a plan featuring specific milestones with obligation and outlay estimates for every system of the agency (both current and under development).

10. Contingency plan and/or disaster recovery plan exists - agencies shall develop, maintain, and test disaster recovery and continuity of operations plans for their data center(s). The plan's objective is to provide reasonable continuity of data processing support if normal operations are prevented.

11. Vulnerability assessment conducted - a review of the susceptibility of a program or function to waste, loss, unauthorized use, or misappropriation. Includes both vulnerability assessments or their equivalents, such as an audit.

12. Cost-benefit analysis exists - a review to determine and compare the benefits of the proposed system against the cost of developing and operating the current system. Only those proposals where the expected benefits exceed the estimated costs by 10 percent should be considered for development, unless otherwise specifically required by statute.

13. Reasonable assurance applied - reasonable assurance equates to a satisfactory level of confidence, based on management's judgment of the cost-benefits of the controls versus the recognized risks. (Practically, it is recognized that it is not cost-effective to attain 100 percent assurance.)

14. Control objectives defined - goals established to address a known vulnerability or promote reliability or security of a system.

15. Control techniques selected - methods to satisfy one or more control objectives by preventing, detecting, and/or correcting undesired events. More commonly referred to as "controls."

16. Adequacy of security requirements determined - agencies shall ensure that the appropriate technical, administrative, physical, and personnel security requirements

are included in specifications for the acquisition or operation of facilities, equipment, or software.

17. Security specifications exist - internal control and security objectives must be stated as design specifications and approved by management before development (programming) of the application system can begin.

18. Adequacy of security specifications determined - proof that the design specifications satisfy control objectives must be presented to management to authorize computer program development and/or modification (programming).

19. System design approved - before development (programming) of the system is authorized, management must be assured that the system design satisfies the user's requirements and incorporates the control requirements. The design review must be documented and be available for examination.

20. Controls documented - internal control systems, 'including all transactions and significant events, are to be clearly documented and be readily available for examination.

21. System documentation exists - documentation that must reflect the current state of the system as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.

22. System contingency plan exists - plans must be developed, documented, and tested to ensure that users of the system can continue to perform essential functions in the event their information technology support is interrupted. The plan should also be consistent with the agencywide disaster recovery plan.

23. Controls tested - before a new or modified system is placed into production status, the controls should be tested to prove that the controls operate as intended. The test results should be documented and sent to management for approval to implement the system.

24. System test conducted - before implementation of the system is authorized, evidence that the system operates as intended must be presented to management. This evidence must also include the results of controls testing. The test results must be documented and available for examination.

25. Test results documented - the documentation should demonstrate that the control and functionality requirements operate as intended.

26. System certified prior to implementation - before a system can be implemented, an agency official shall certify that

the system meets all applicable Federal policies, regulations, and standards, as well as state that test results demonstrate that installed controls are adequate for examination.

27. Controls review performed - periodically, the controls of each system must be tested to determine if the controls still function as intended. The results of these tests “ must be documented and available for examination.

28. Periodic reviews and recertification are conducted at least every 3 years, agencies shall review applications and recertify the adequacy of the safeguards. The recertification shall be documented and be available for review.

29. Periodic risk assessments are conducted - agencies shall conduct periodic risk assessments at each data center to provide a measure of the relative vulnerabilities and threats to the data center so that security resources can be effectively distributed to minimize potential loss.

30. Corrective action taken; audit findings resolved promptly - managers are to promptly evaluate audit findings and recommendations, determine proper corrective actions, and complete those actions.

31. Annual report on internal controls prepared - yearly, each agency must determine if its systems of internal controls are in compliance with the Comptroller General’s standards.

32. Annual report on accounting systems prepared - yearly, each agency must determine if its accounting systems are in compliance with the Comptroller General’s standards.

33. Annual reports to President sent - the head of each agency must sign both annual reports and transmit them to both the President and Congress.

- ADMINISTRATIVE CONTROLS

34. Organizational responsibility is affixed - the assignment of responsibilities for planning, directing and controlling the controls evaluation process for the agency and/or segment is specified. The programs and functions conducted in each of the components have also been specified.

35. Separation of duties exists - key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

36. Supervision is provided - qualified and continuous supervision is to be provided to ensure that control requirements are met.

37. Supportive attitudes exist - managers and employees are to maintain and demonstrate a positive and supportive attitude toward controls at all times.

38. Personnel are competent - managers and employees are to have personal and professional integrity and are to maintain a level of competence that allow them to accomplish their assigned duties, as well as understand the importance of developing and implementing good controls.

39. Security training program exists - agencies shall establish a security awareness and training program so that agency and contractor personnel involved with information systems are aware of their security responsibilities and know how to fulfill them.

40. Written policies and procedures exist - each agency shall establish administrative procedures to enforce the intended functioning of controls, including provisions that performance appraisals reflect execution of control-related responsibilities.

41. Personnel security policies exist "- each agency should establish and manage personnel security procedures, including requirements for screening agency and contractor personnel designing, developing, operating, maintaining, or using the system. The level of screening depends on the sensitivity and/or classification of the system data.

42. Individual responsibilities are affixed - assignments of responsibility should be made for internal controls, accounting systems, and data center security on an agencywide and individual system and/or center basis.

43. Custody and/or accountability assigned - the official whose function is supported by an information system is responsible and accountable for the products of the information system.

44. Record disposition procedures exist - each agency must establish approved records disposition schedules which identify permanent data files and ensure their transfer to the National Archives and Record Administration.

45. Release of information provided for - each agency must have procedures in place so that information can be extracted from systems to meet requests made under the Privacy Act and the Freedom of Information Act.

- **REQUIRED SYSTEM FUNCTIONS**

46. An analysis of the ratio of outputs to inputs evaluated against an acceptable standard.

47. System operation is economical - uneconomical systems must be identified and phased out.

48. System is effective - periodically, each system should be reviewed to determine if the system still meets organizational needs.

49. System supports management - data shall be recorded and reported in a manner to facilitate carrying out the responsibilities of both program and administrative managers.

50. System supports budget - financial management data shall be recorded, stored, and reported to facilitate budget preparation, analysis, and execution.

51. Comparability and/or consistency provided for - financial management data shall be recorded and reported in the same manner throughout the agency, using uniform definitions that are synchronized with budgeting and used consistently for each reporting period.

52. Information is useful and/or relevant - data capture and reports shall be tailored to specific user needs, and if usage does not justify costs, data or reports shall be terminated.

53. System provides full disclosure - data shall be recorded and reported to provide users of the data with complete information about the subject of the report per OMB, Treasury, and Privacy Act *standards.*

54. Individual access allowed - systems must be able to extract any data contained in the data base about individuals to meet requests to see the data by that individual or his/her representative when required by the Privacy Act.

55. Network compatibility exists - any systems developed or acquired must be interoperable with any existing system that will be linked to the new system.

C. CROSS-REFERENCE TO CONTROL DIRECTIVES

Table 3-1 on page 3-7 provides a listing of the 55 control requirements cross-referenced to the major control directives cited in Chapter 2.

Table 3.1 Summary table of control objectives cross-referenced to the major control directives.

Line						GAO		Privacy	DoD	DoD
No.	Requirements	A-123	OMB IC	A-127	A-130	Title II	FMFIA	Act	IMCP	IRMP
	Application Controls									
1.	Transactions are authorized	X	X		X	X		X		
2.	Transactions are valid	x	X		X	X	X			
3.	Information is complete	X	X	X		“X	X	X		X
4.	Information is accurate	X	X	X	X	X	X	X		X
5.	Information is timely	x	X	X		X	X	X		X
6.	System and data are secure				X		X	X		X
7.	System is auditable			X		X				
	General Controls									
8.	System controls exist				X	X				
9.	5-year system plan developed			X	X	X			X	
10.	Contingency plan/organization disaster recovery plan exists				X	X				X
11.	Vulnerability assessment conducted	x	X			X			X	
12.	Cost/benefit analysis exists					X				X
13.	Reasonable assurance applied	x	X	X	X	X	X		X	
14.	Control objectives defined	X	X			X			X	
15.	Control techniques selected	X	X			X			X	
16.	Adequacy of security requirements determined				X					
17.	Security specifications exist				X	X				X
18.	Adequacy of security specifications determined				X					
19.	System design approved				X	X				
20.	Controls documented	x	X			X				
21.	System documentation exists					X				
22.	System contingency plan exists				X	X				
23.	Controls tested				X	X				
24.	System test conducted					X				
25.	Test results documented				X	X				
26.	System certified prior to implementation				X					
27.	Controls review performed	X	X	X		X	X			
28.	Periodic reviews and recertification are conducted			X	X	X			X	X

Table 3.1 **Continued-Summary** table **of** control objectives **cross--referenced** to the major control directives.

29. Periodic risk assessments are conducted				X	X			X	
30. Corrective action taken; audit findings resolved promptly	X	X	“		X			X	
31. Annual report on internal controls prepared			X	X		X		X	
32. Annual report on amounting systems prepared					X	X		X	
33. Annual reports sent to President	X	X		X	X	X		X	
Administrative Controls									
34. Organizational responsibility is affixed		X						X	X
35. Separation of duties exist	X	X			X			X	
36. Supervision is provided	X	X			X			X	
37. Supportive attitudes exist	X	“ X			X			X	
38. Personnel are competent	X	X			X			X	
39. Security training program exists				X				X	
40. Written policies and procedures exist	X	X	X					X	X
41. Personnel security policies exists				X				X	
42. Individual responsibilities are affixed	X	X	X	X	X			X	
43. Custody/accountability assigned	X	X		X	X	X		X	X
44. Record retention procedures exist							X		X
45. Release of information is provided for							X	X	X
Required System Functions									
46. System is efficient			X		X				X
47. System operation is economical			X		X				
48. System is effective				X	X				X
49. System supports management			X					X	X
50. System supports budget			X		X			X	
51. Comparability/consistency provided for			X		X				
52. Information is useful/relevant			X	X	X		X		X
53. System provides full disclosure			X		X		X		
54. Individual access allowed				X		X	X		
55. Network compatibility exists				X					